

Technicien d'infrastructures numériques durables, sécurisées et responsables

RNCP41773 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 5
Code(s) NSF	326, 326r
Formacode(s)	31051, 31002, 31006, 12522
Code(s) ROME	I1401, M1801
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	18/12/2025
Date d'échéance	18/12/2028

Certificateur(s)

GEFI · SIRET : 41262676400028

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le développement numérique transforme en profondeur nos sociétés, posant des questions fondamentales sur la place de l'humain dans un écosystème technologique en constante mutation. Dans ce contexte, le technicien d'infrastructures numériques durables, sécurisées et responsables intervient au service des utilisateurs – qu'ils soient usagers, clients, patients, collègues, commanditaires ou supérieurs – au sein d'organisations publiques ou privées, quels que soient leur taille ou leur secteur d'activité.

Le technicien intervient dans une imminence de maturité numérique responsable, anticipant les évolutions technologiques, intégrant les enjeux de sécurité, d'automatisation, d'accessibilité, de sobriété numérique, de développement durable.

ACTIVITÉS VISÉES

Diagnostiquer et résoudre des dysfonctionnements, avec des solutions adaptées et innovantes ;

Installer, configurer, déployer et maintenir des infrastructures numériques durables et sécurisées ;

Informar, sensibiliser, accompagner, conseiller et former les utilisateurs, en français et dans une langue étrangère (niveau B1 CECRL) ;

Utiliser des technologies de pointe et s'appuyer sur des approches d'apprentissage centrées sur l'utilisateur ;

Assurer une veille technologique, technique, réglementaire et légale.

COMPÉTENCES ATTESTÉES

Analyser les incidents et dysfonctionnements techniques survenant au sein d'une infrastructure numérique, en mobilisant des méthodes de diagnostic efficaces et innovantes.

Identifier les causes racines et les difficultés techniques associées, en mobilisant des méthodes de diagnostic efficaces et innovantes.

Évaluer les impacts multiples d'un incident mineur, majeur, critique :

- techniques (pannes, indisponibilités, atteinte à la performance),
- énergétiques (consommation excessive, redondances inutiles),
- économiques et tarifaires (coûts directs et indirects pour l'organisation ou l'utilisateur).

Surveiller les indicateurs de performance et de santé de l'infrastructure numérique en installant et exploitant des outils de supervision détectant des anomalies mineures à majeures, exploitant des solutions d'intelligence

artificielle prédictives de pannes.

Traiter les alertes de sécurité, en identifiant la nature de l'événement et évaluer le niveau de criticité du risque cyber (mineur, majeur, critique), en mobilisant des mesures préventives ou correctives.

Définir et exploiter des indicateurs pertinents pour la supervision d'une infrastructure numérique, en distinguant les alertes mineures (niveau d'information ou de surveillance) des alertes majeures (nécessitant une action immédiate ou une escalade).

Documenter avec rigueur l'ensemble des diagnostics, incidents traités, hypothèses posées, solutions apportées et recommandations formulées, en respectant les bonnes pratiques de traçabilité.

Communiquer de manière claire, graduée et adaptée auprès d'un·e utilisateur, notamment sur les incidents et les solutions, en tenant compte de leur profil technique, du niveau d'urgence, et en utilisant des supports adaptés.

Assurer une veille continue et proactive sur :

- les technologies et outils de diagnostic et de supervision,
- les vulnérabilités connues, les menaces émergentes,
- les retours d'expérience professionnels,
- les exigences réglementaires et les normes en vigueur (RGPD, ISO/IEC 27001, référentiels RSE, éco-conception...).

Installer et configurer les composants d'une infrastructure numérique,

en assurant l'interopérabilité avec l'existant, quelles que soient les contraintes.

Maintenir une infrastructure numérique en conditions opérationnelles, en apportant des mesures curatives et préventives, et, en assurant la continuité de service, la sécurité des systèmes et la performance des équipements, tout au long de leur cycle de vie.

Déployer une infrastructure numérique, en intégrant les contraintes organisationnelles, énergétiques, économiques et réglementaires spécifiques à chaque environnement (infrastructures locales, distantes ou hybrides).

Mettre en œuvre des solutions techniques durables, en assurant l'écoresponsabilité d'une infrastructure numérique fondée sur des critères d'éco-conception, de sobriété numérique, de réparabilité, de recyclabilité,...

Mettre en œuvre des solutions dématérialisées et hybrides, en intégrant des services privilégiant la virtualisation, telles que l'utilisation de services cloud, d'environnements virtualisés, de technologies containerisées, en tenant compte des contraintes de sécurité, d'accessibilité et d'optimisation des ressources.

Mettre en œuvre des solutions automatisées afin de standardiser, sécuriser et optimiser les installations, maintenances et configurations.

Appliquer les règles de cybersécurité et de conformité, en installant, maintenant, déployant des mesures de sécurité, dans le respect des lois et/ou réglementations en vigueur.

Surveiller et optimiser les indicateurs de performance, en distinguant les indicateurs mineurs (tendances, seuils d'alerte anticipables) et majeurs voire critiques nécessitant une action immédiate, dans une perspective d'amélioration continue.

Consigner l'ensemble des actions et paramètres dans une documentation technique rigoureuse, constituant un référentiel de base au système d'information, y compris les informations confidentielles, en garantissant leur traçabilité, leur sécurité et leur accessibilité aux interlocuteur·rice·s autorisé·e·s.

Communiquer de manière appropriée, graduée et contextualisée avec les utilisateurs y compris les parties prenantes, en adaptant le niveau de technicité du discours, les supports et les modalités de transmission.

Assurer une veille active et multidimensionnelle sur :

- les innovations techniques et outils de déploiement ou maintenance,
- les vulnérabilités émergentes et menaces cyber,
- les retours d'expérience, pratiques professionnelles et benchmarks,
- les obligations réglementaires, normes (ISO, RGPD, RSE...) et bonnes pratiques en lien avec les infrastructures numériques responsables.

Gérer le flux des demandes courantes et variées des utilisateurs, qu'elles soient formulées sur site ou à distance, en identifiant les priorités, en catégorisant les incidents et en appliquant des procédures adaptées selon la nature et la criticité des sollicitations.

Prendre en charge les demandes courantes (assistance à l'utilisation, résolution de pannes simples, aide à la configuration...), en assurant une intervention rapide, pertinente et respectueuse de l'autonomie des utilisateurs.

Communiquer de manière claire, graduée et adaptée, en tenant compte du niveau de maîtrise numérique de chaque interlocuteur, de ses besoins spécifiques (y compris en situation de handicap), et du contexte d'usage (poste de travail, environnement distant, mobile...).

Conseiller, orienter et sensibiliser les utilisateurs vers des solutions responsables (éco-gestes numériques, sécurité

des données, bonnes pratiques...), tout en valorisant l'usage efficace, éthique et durable des outils numériques mis à disposition.

Mesurer, analyser et exploiter les indicateurs de fonctionnement, en distinguant les indicateurs mineurs, des indicateurs majeurs et critiques, dans une démarche d'adaptation continue aux usages.

Préparer des supports techniques et de communication, tels que des fiches de procédure, Foires Aux Questions (FAQ), guides utilisateurs, tutoriels, supports de formation, ateliers,... en assurant leur lisibilité, leur accessibilité (selon les standards WCAG, par exemple), et leur pertinence selon les profils.

Participer à l'amélioration continue du système d'information, en remontant les retours d'usage, les dysfonctionnements récurrents, les besoins d'évolution ou de formation identifiés, et en proposant des solutions ou recommandations opérationnelles innovantes et responsables.

Blocs de compétences

RNCP41773BC01 — Diagnostiquer et analyser une infrastructure numérique durable, sécurisée et responsable

LISTE DE COMPÉTENCES

Analyser les incidents et dysfonctionnements techniques survenant au sein d'une infrastructure numérique, en mobilisant des méthodes de diagnostic efficaces et innovantes.

Identifier les causes racines et les difficultés techniques associées, en mobilisant des méthodes de diagnostic efficaces et innovantes.

Évaluer les impacts multiples d'un incident mineur, majeur, critique :

- techniques (pannes, indisponibilités, atteinte à la performance),
- énergétiques (consommation excessive, redondances inutiles),
- économiques et tarifaires (coûts directs et indirects pour l'organisation ou l'utilisateur).

Surveiller les indicateurs de performance et de santé de l'infrastructure numérique en installant et exploitant des outils de supervision détectant des anomalies mineures à majeures, exploitant des solutions d'intelligence artificielle prédictives de pannes.

Traiter les alertes de sécurité, en identifiant la nature de l'événement et évaluer le niveau de criticité du risque cyber (mineur, majeur, critique), en mobilisant des mesures préventives ou correctives.

Définir et exploiter des indicateurs pertinents pour la supervision d'une infrastructure numérique, en distinguant les alertes mineures (niveau d'information ou de surveillance) des alertes majeures (nécessitant une action immédiate ou une escalade).

Documenter avec rigueur l'ensemble des diagnostics, incidents traités, hypothèses posées, solutions apportées et recommandations formulées, en respectant les bonnes pratiques de traçabilité.

Communiquer de manière claire, graduée et adaptée auprès d'un utilisateur, notamment sur les incidents et les solutions, en tenant compte de leur profil technique, du niveau d'urgence, et en utilisant des supports adaptés.

Assurer une veille continue et proactive sur :

- les technologies et outils de diagnostic et de supervision,
- les vulnérabilités connues, les menaces émergentes,
- les retours d'expérience professionnels,
- les exigences réglementaires et les normes en vigueur (RGPD, ISO/IEC 27001, référentiels RSE, éco-conception, etc.).

MODALITÉS D'ÉVALUATION

Étude de cas contextualisée, suivie d'une préparation et d'une soutenance orales.

RNCP41773BC02 — Maintenir et déployer une infrastructure numérique durable, sécurisée et responsable

LISTE DE COMPÉTENCES

Installer et configurer les composants d'une infrastructure numérique, en assurant l'interopérabilité avec l'existant, quelles que soient les contraintes.

Maintenir une infrastructure numérique en conditions opérationnelles, en apportant des mesures curatives et préventives, et, en assurant la continuité de service, la sécurité des systèmes et la performance des équipements, tout au long de leur cycle de vie.

Déployer une infrastructure numérique, en intégrant les contraintes organisationnelles, énergétiques, économiques et

réglementaires spécifiques à chaque environnement (infrastructures locales, distantes ou hybrides).

Mettre en œuvre des solutions techniques durables, en assurant l'écoresponsabilité d'une infrastructure numérique fondée sur des critères d'éco-conception, de sobriété numérique, de réparabilité, de recyclabilité,...

Mettre en œuvre des solutions dématérialisées et hybrides, en intégrant des services privilégiant la virtualisation, telles que l'utilisation de services cloud, d'environnements virtualisés, de technologies containerisées, en tenant compte des contraintes de sécurité, d'accessibilité et d'optimisation des ressources.

Mettre en œuvre des solutions automatisées afin de standardiser, sécuriser et optimiser les installations, maintenances et configurations.

Appliquer les règles de cybersécurité et de conformité, en installant, maintenant, déployant des mesures de sécurité, dans le respect des lois et/ou réglementations en vigueur.

Surveiller et optimiser les indicateurs de performance, en distinguant les indicateurs mineurs (tendances, seuils d'alerte anticipables) et majeurs voire critiques nécessitant une action immédiate, dans une perspective d'amélioration continue.

Consigner l'ensemble des actions et paramètres dans une documentation technique rigoureuse, constituant un référentiel de base au système d'information, y compris les informations confidentielles, en garantissant leur traçabilité, leur sécurité et leur accessibilité aux interlocuteurs autorisés.

Communiquer de manière appropriée, graduée et contextualisée avec les utilisateurs y compris les parties prenantes, en adaptant le niveau de technicité du discours, les supports et les modalités de transmission.

Assurer une veille active et multidimensionnelle sur :

- les innovations techniques et outils de déploiement ou maintenance,
- les vulnérabilités émergentes et menaces cyber,
- les retours d'expérience, pratiques professionnelles et benchmarks,
- les obligations réglementaires, normes (ISO, RGPD, RSE...) et bonnes pratiques en lien avec les infrastructures numériques responsables.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle, réelle ou simulée, qui permet d'observer le candidat en action sur des tâches d'installation, de configuration ou de maintenance d'infrastructures.

RNCP41773BC03 — Participer à la mutation d'une infrastructure numérique durable, sécurisée et responsable

LISTE DE COMPÉTENCES

Gérer le flux des demandes courantes et variées des utilisateurs, qu'elles soient formulées sur site ou à distance, en identifiant les priorités, en catégorisant les incidents et en appliquant des procédures adaptées selon la nature et la criticité des sollicitations.

Prendre en charge les demandes courantes (assistance à l'utilisation, résolution de pannes simples, aide à la configuration, etc.), en assurant une intervention rapide, pertinente et respectueuse de l'autonomie des utilisateurs.

Communiquer de manière claire, graduée et adaptée, en tenant compte du niveau de maîtrise numérique de chaque interlocuteur de ses besoins spécifiques (y compris en situation de handicap), et du contexte d'usage (poste de travail, environnement distant, mobile, etc.).

Conseiller, orienter et sensibiliser les utilisateurs vers des solutions responsables (écogestes numériques, sécurité des données, bonnes pratiques, etc.), tout en valorisant l'usage efficace, éthique et durable des outils numériques mis à disposition.

Mesurer, analyser et exploiter les indicateurs de fonctionnement, en distinguant les indicateurs mineurs, des indicateurs majeurs et critiques, dans une démarche d'adaptation continue aux usages.

Préparer des supports techniques et de communication, tels que des fiches de procédure, Foires Aux Questions (FAQ), guides utilisateurs, tutoriels, supports de formation, ateliers, etc. en assurant leur lisibilité, leur accessibilité (selon les standards WCAG, par exemple), et leur pertinence selon les profils.

Participer à l'amélioration continue du système d'information, en remontant les retours d'usage, les dysfonctionnements récurrents, les besoins d'évolution ou de formation identifiés, et en proposant des solutions ou recommandations opérationnelles innovantes et responsables.

MODALITÉS D'ÉVALUATION

Mise en situation d'assistance utilisateur sous forme de jeu de rôle interactif.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le technicien d'infrastructures numériques durables, sécurisées et responsables intervient au service des utilisateurs – qu'ils soient usagers, clients, patients, collègues, commanditaires ou supérieurs – au sein d'organisations publiques ou privées, quels que soient leur taille ou leur secteur d'activité.

TYPE D'EMPLOIS ACCESSIBLES

Technicien Green & Safe IT / Green IT - Technicien d'infrastructure numérique responsable / de maintenance informatique / de déploiement informatique / d'exploitation informatique / informatique

Technicien support utilisateur - Technicien Système & Réseau informatiques / Système informatique / Réseau informatique / Informatique & Téléphonie / Informatique & Solutions d'impression - Technicien Installateur Informatique

Technicien Green & Safe Hardware / Software - Technicien / Conseiller Data Center - Conseiller de vente High Tech / Informatique - Conseiller de SAV High Tech

Assistant Manager Green IT / Green & Safe IT - Assistant Responsable Green IT / Safe Green IT - Assistant Administrateur d'infrastructure numérique responsables - Assistant Manager / Responsable Data Center

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier n'est pas réglementé en tant que tel mais ce technicien se doit de prendre en compte les contraintes légales et réglementaires liées à l'exercice des activités du métier.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Modérée (3/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 4 sur 5.
Facteurs principaux	Intensité d'embauche, Inadéquation géographique
Salaire médian (mensuel)	2 419 €
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée)
Projets de recrutement (BMO 2026)	9 549
Jugés difficiles à recruter	46 %
Emplois saisonniers	3 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

L'accès à la certification professionnelle ou à l'un ou deux blocs de compétences est destiné à tout candidat en mutation professionnelle dans le domaine de la maintenance informatique, en particulier intéressé par le numérique responsable, autrement dit Green & Safe IT.

Aucun prérequis de niveau de qualification.

Ouvert à la Validation d'Acquis de l'Expérience (VAE).

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE

PROFESSIONNALISATION, CANDIDATURE INDIVIDUELLE

Le jury comprend au minimum 5 membres, dont 3 membres extérieurs issus du monde professionnel (soit 60 % de membres extérieurs). Le président du jury est un expert du secteur (cadre informatique ou technicien supérieur justifiant d'une expérience confirmée dans le domaine).

COMPOSITION DU JURY — VAE

Jury de 5 membres, dont au moins 3 externes (techniciens, responsables informatiques, experts infrastructures, etc.).

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	7 714 €
Selon la branche	6 500 € – 8 146 €

Prise en charge	Branches concernées
7 714 €	Valeur par défaut · 205 branches
8 146 €	CPNE autoroutes, CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
8 135 €	CPNEF de l'audiovisuel
8 036 €	CPNEFP dans les établissements d'enseignement privés sous contrat
8 018 €	CPNEFP ICGV entreprises de la viande
7 918 €	CPNE des Télécoms
6 500 €	CPNE Branche Caoutchouc

Base légale

Date de décision	18/12/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	18/12/2028
Date de dernière délivrance possible	18/12/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	88	1	82 %	—
2023	127	0	88 %	80 %
2022	176	0	93 %	75 %
2021	133	0	91 %	83 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP37079

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41773/>